EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://prorecurrencia.transfiriendo.com	Checks	9 pruebas
Dominio	prorecurrencia.transfiriendo.com	Hallazgos	15 totales
Fecha	13 de mayo de 2026 a las 16:20	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio prorecurrencia.transfiriendo.com arroja una puntuación técnica de 73/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó exitoso, 1 presentó un fallo directo y el resto no pudo ser verificado debido a errores de conexión en el servidor. La imposibilidad de validar el cifrado de datos y las cabeceras de protección representa una brecha crítica en la infraestructura. Por lo tanto, el sitio se clasifica actualmente como vulnerable y requiere intervención inmediata para garantizar la integridad de la información.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión segura con el servidor, lo que impide el cifrado de la información y expone los datos de los usuarios a interceptaciones.
[LOW] Fallo en robots.txt: No se pudo acceder al archivo de directrices de rastreo, lo que puede provocar una indexación ineficiente o exposición involuntaria de rutas.
[LOW] Fallo en sitemap.xml: El mapa del sitio no está disponible o es inaccesible, dificultando la auditoría de la estructura jerárquica de la web.
[INFO] Indisponibilidad de cabeceras: El servidor no respondió a las solicitudes de verificación de cabeceras de seguridad, cookies y redirecciones, lo que sugiere una configuración de red restrictiva o incorrecta.